



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/881,921	06/14/2001	Gerald Francis McBrearty	AUS920010388US1	8362

35525 7590 04/28/2005

IBM CORP (YA)
C/O YEE & ASSOCIATES PC
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER

MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 04/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/881,921	Applicant(s) MCBREARTY ET AL.	
	Examiner Aravind K. Moorthy	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 January 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3,4,7-11,13,14,17-21,23,24 and 27-30 is/are pending in the application.
- 4a) Of the above claim(s) 2,5,6,12,15,16,22,25 and 26 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3,4,7-11,13,14,17-21,23,24 and 27-30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11 September 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is in response to the amendment filed on 29 December 2004.
2. Claims 1, 3, 4, 7-11, 13, 14, 17-21, 23, 24 and 27-30 are pending in the application.
3. Claims 1, 3, 4, 7-11, 13, 14, 17-21, 23, 24 and 27-30 have been rejected.
4. Claims 2, 5, 6, 12, 15, 16, 22, 25 and 26 have been cancelled.

Response to Amendment

5. The examiner approves the amendment made to the specification. The applicant has corrected the typographical error. No new matter has been added.

Response to Arguments

6. Applicant's arguments with respect to claims 1, 3, 4, 7-11, 13, 14, 17-21, 23, 24 and 27-30 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the

Art Unit: 2131

reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

7. Claims 1, 3, 4, 11, 13, 14, 21, 23 and 24 are rejected under 35 U.S.C. 102(e) as being anticipated by Burns et al U.S. Patent No. 6,405,315 B1.

The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

As to claims 1, 11 and 21, Burns et al discloses a computer-implemented method of encrypting data, the data being comprised of a plurality of data chunks, comprising:

encrypting a first data chunk [column 8, lines 5-20];

calculating an intermediate digital digests for the first encrypted data chunk [column 8, lines 5-20];

repeating the encrypting and calculating steps for each data chunk of the plurality of data chunks thereby creating a plurality of encrypted data chunks and associated intermediate digital digests [column 8, lines 5-20]; and

formulating a data package comprising the encrypted data chunks and the plurality of intermediate digital digests [column 8, lines 5-20].

As to claims 3, 13 and 23, Burns et al discloses that each intermediate digital digest builds from a previously calculated intermediate digital digest [column 8, lines 5-20].

As to claims 4, 14 and 24, Burns et al discloses a computer-implemented method of decrypting an encrypted data package, the encrypted data package being comprised of a plurality of encrypted data portions and a plurality of encrypted intermediate digital digests, wherein each encrypted data portion corresponds to an encrypted intermediate digital digest, comprising:

reading an encrypted data portion from the plurality of encrypted data portions [column 8, lines 5-20];

calculating a digital digest for the encrypted data portion [column 8, lines 5-20];

decrypting an intermediate digital digest corresponding to the encrypted data portion from the plurality of intermediate digital digests [column 8, lines 21-27];

authenticating the encrypted data portion based on a comparison of the decrypted intermediate digital digest to the calculated digital digest [column 8, lines 5-20]; and

in response to a match decrypting the encrypted data portion and repeating the reading, calculating, decrypting and authenticating steps for a next encrypted data portion of the data package [column 8, lines 5-20].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2131

8. Claims 7, 17 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burns et al U.S. Patent No. 6,405,315 B1 as applied to claims 4, 14 and 24 above, and further in view of Zhang U.S. Patent No. 6,154,541.

As to claims 7, 17 and 27, Burns et al does not teach that in response to a mis-match of the decrypted intermediate digital digest and the calculated digital digest, discarding the encrypted data package.

Zhang teaches discarding a decrypted digital digest in response to a mis-match [column 36, lines 33-60].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Burns et al so that if a mis-match occurred for the decrypted intermediate digital digest and the calculated digital digest, the encrypted data package would have been discarded.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Burns et al by the teaching of Zhang because by discarding the mis-matched data, it gets rid of data that has been altered by a third party.

9. Claims 8-10, 18-20 and 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Burns et al U.S. Patent No. 6,405,315 B1 as applied to claims 4, 14 and 24 above, and further in view of Kawamae et al U.S. Patent No. 6,850,954 B2.

As to claims 8, 9, 18, 19, 28 and 29, Burns et al teaches decrypting an intermediate digital digest includes reading the intermediate digital digest from a digital digest portion of the encrypted data package [column 10, lines 21-41].

Burns et al does not teach that the digital digest portion has the plurality of intermediate digital digests arranged in an order [column 5 line 11 to column 6 line 37]. Burns et al does not teach that the intermediate digital digest is built up from a previous intermediate digital digest in the order [column 5 line 11 to column 6 line 37].

Kawamae et al teaches a digital digest portion that has the plurality of intermediate digital digests arranged in an order. Kawamae et al teaches that the intermediate digital digest is built up from a previous intermediate digital digest in the order.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Burns et al so that the digital digest portion would have had the plurality of digital digests arranged in a particular order. The intermediate digital digest would have been built up from a previous intermediate digital digest in the order.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Burns et al by the teaching of Kawamae et al because having the digital digests in a particular order, it facilitates for searches and arranging of keywords [column 1, lines 48-62].

As to claims 10, 20 and 30, Burns et al teaches that the intermediate digital digest corresponds to a different amount of encrypted data than other intermediate digital digests in the digital digest portion [column 8, lines 5-20].

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


Art Unit: 2131


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy 
April 19, 2005


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100